Advanced Cryptography: Lightweight Cryptography

MICHAEL NÜSKEN, DANIEL LOEBENBERGER

9. Exercise sheet
Hand in solutions until Monday, 16 January 2012, 23:59:59.

If you find any errors in the sheets, do not hesitate to write an email to the mailing list `11ws-ac@lists.bit.uni-bonn.de`.

Exercise 9.1 (SHA-3 candidates). (10 points)

On the website `http://csrc.nist.gov/groups/ST/hash/sha-3/Round3/submissions_rnd3.html` you find the five SHA-3 finalists. Give a justified recommendation which one you find best suitable for lightweight applications. Furthermore compare your selection to the PRESENT-based constructions of hash functions in terms of speed, space-requirements and security. /10

Exercise 9.2. (15+5 points)

Implement DM-PRESENT-80. Find a collision. 15+5

Why is your collision not a security threat in lightweight scenarios?